EXHIBIT A

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

MAXELL HOLDINGS, LTD., *Plaintiff,* v. AMPEREX TECHNOLOGY LIMITED, *Defendant.*	CIVIL ACTION NO. 6:21-cv-347-ADA

DECLARATION OF FANGHUA LIU REGARDING
DATA SECURITY LAW OF THE PEOPLE'S REPUBLIC OF CHINA

I, Fanghua Liu, declare as follows:

1. I am an attorney duly licensed to practice law in the People's Republic of China.
2. I am a Partner of the law firm of Lecome Law firm.
3. I submit this declaration to discuss the newly enacted Data Security Law of the People's Republic of China, effective on September 1, 2021 ("PRC Data Security Law"). A copy of the law is herein attached as Exhibit 1. A copy of the certified translation of the law is herein attached as Exhibit 2. I have personal knowledge of the facts stated herein, and all facts stated are true and correct, to the best of my knowledge.
4. As relevant to this litigation, according to Article 36 of the PRC Data Security Law, no

organization or individual within the territory of the People's Republic of China may provide foreign judicial or law enforcement authorities with the data stored within the territory of the People's Republic of China without the approval of the competent authorities of the People's Republic of China. Article 36, PRC Data Security Law, effective September 1, 2021.

5. "Data" as used in the law refers to any recording of information by electronic or other means. Article 3, PRC Data Security Law, effective September 1, 2021.
6. It is my opinion that the PRC Data Security Law applies to ATL in this litigation.
7. Consequently, it is further my opinion that, without the express approval from the authorities of the PRC, ATL would risk violating this law should ATL provide this Court or Plaintiff with any data that is stored within the territory of China, including, but not limited to, confidential material relating to the operation of ATL's lithium ion battery products.
8. There are serious penalties for violating the PRC Data Security Law which include a fine not less than 100,000 yuan, the person directly in charge and other directly liable persons may be fined not less than 10,000 yuan; if serious consequences are caused, a fine of not less than 1 million yuan will be imposed, and the organization may be ordered to suspend the relevant business, suspend the operation for rectification, or its relevant business permit or business license will be revoked, and the person directly in charge and other directly liable persons will be fined not less than 50,000 yuan.
9. It is my understanding and observation that various authorities in China are in the process of establishing their review procedures for any data exportation request. Until and unless those procedures are established and ATL's data exportation request is approved by the

relevant Chinese authorities can ATL comply with this Court's rules, without risking significant sanctions from the Chinese government.

10. It is my understanding that on Aug. 30 and 31, ATL requested guidance from NingDe Cyberspace Administration, Cyberspace Administration of China, and Intellectual Property Bureau of NingDe City regarding its obligations under the PRC Data Security Law and its requirements in this litigation.

I declare under penalty of perjury under the laws of the United States and the State of Texas that the foregoing is true and correct.

September 8, 2021

By: Fanghua Liu

Fanghua Liu

EXHIBIT 1

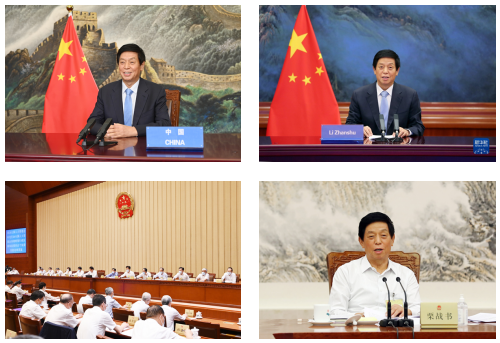
中华人民共和国数据安全法

（2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过）

来源： 中国人大网 浏览字号： 大 中 小 2021年06月10日 19:58:46

目 录

图片报道 更多>>



立法 >>

- 全国人大宪法和法律委员会赴黑龙...
- 新修改的安全生产法施行 多地对违...
- 我们需要什么样的家庭教育立法
- 慈善法实施5周年 这些问题你是否...
- 土地管理法实施条例9月1日起正式...

监督 >>

- 人大代表建议加大对骗取公证文书...
- 全国人大常委会公证法执法检查组...

第七章 附 则

第一章 总 则

第一条 为了规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益，制定本法。

第二条 在中华人民共和国境内开展数据处理活动及其安全监管，适用本法。

在中华人民共和国境外开展数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

第三条 本法所称数据，是指任何以电子或者其他方式对信息的记录。

数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

第四条 维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

第五条 中央国家安全领导机构负责国家数据安全工作的决策和议事协调，研究制定、指导实施国家数据安全战略和有关重大方针政策，统筹协调国家数据安全的重大事项和重要工作，建立国家数据安全工作协调机制。

第六条 各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责。

- 切实加强地方人大对政府债务的审...
- 为人大财经干部更好履职强基础、...
- 公证服务要解民难化民忧安民心

代表 >>

- 守护“高原精灵”
- 陈恩明：推行农机社会化服务&ens...
- 王士岭：立足本职守初心
- 何菲：“梦桃精神”，代代相传！
- 开学第一课，拉齐尼的儿女唱起他...

专题集锦 >>

- 习近平新时代中国特色社会主义思...
- 学习习近平总书记关于民法典重要...
- 全过程人民民主
- 建党百年 新时代人大工作巡礼
- 个人信息保护法立法

工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。

公安机关、国家安全机关等依照本法和有关法律、行政法规的规定，在各自职责范围内承担数据安全监管职责。

国家网信部门依照本法和有关法律、行政法规的规定，负责统筹协调网络数据安全和相关监管工作。

第七条 国家保护个人、组织与数据有关的权益，鼓励数据依法合理有效利用，保障数据依法有序自由流动，促进以数据为关键要素的数字经济发展。

第八条 开展数据处理活动，应当遵守法律、法规，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，履行数据安全保护义务，承担社会责任，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

第九条 国家支持开展数据安全知识宣传普及，提高全社会的数据安全保护意识和水平，推动有关部门、行业组织、科研机构、企业、个人等共同参与数据安全保护工作，形成全社会共同维护数据安全和促进发展的良好环境。

第十条 相关行业组织按照章程，依法制定数据安全行为规范和团体标准，加强行业自律，指导会员加强数据安全保护，提高数据安全保护水平，促进行业健康发展。

第十一条 国家积极开展数据安全治理、数据开发利用等领域的国际交流与合作，参与数据安全相关国际规则和标准的制定，促进数据跨境安全、自由流动。

第十二条 任何个人、组织都有权对违反本法规定的行为向有关主管部门投诉、举报。收到投诉、举报的部门应当及时依法处理。

有关主管部门应当对投诉、举报人的相关信息予以保密，保护投诉、举报人的合法权益。

第二章　数据安全与发展

第十三条　国家统筹发展和安全，坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。

第十四条　国家实施大数据战略，推进数据基础设施建设，鼓励和支持数据在各行业、各领域的创新应用。

省级以上人民政府应当将数字经济发展纳入本级国民经济和社会发展规划，并根据需要制定数字经济发展规划。

第十五条　国家支持开发利用数据提升公共服务的智能化水平。提供智能化公共服务，应当充分考虑老年人、残疾人的需求，避免对老年人、残疾人的日常生活造成障碍。

第十六条　国家支持数据开发利用和数据安全技术研究，鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系。

第十七条　国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责，组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。

第十八条 国家促进数据安全检测评估、认证等服务的发展，支持数据安全检测评估、认证等专业机构依法开展服务活动。

国家支持有关部门、行业组织、企业、教育和科研机构、有关专业机构等在数据安全风险评估、防范、处置等方面开展协作。

第十九条 国家建立健全数据交易管理制度，规范数据交易行为，培育数据交易市场。

第二十条 国家支持教育、科研机构和企业等开展数据开发利用技术和数据安全相关教育和培训，采取多种方式培养数据开发利用技术和数据安全专业人才，促进人才交流。

第三章 数据安全制度

第二十一条 国家建立数据分类分级保护制度，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对数据实行分类分级保护。国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。

关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度。

各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。

第二十二条 国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制。国家数据安全工作协调机制统筹协调有关部门加强数据安全风险信

息的获取、分析、研判、预警工作。

第二十三条 国家建立数据安全应急处置机制。发生数据安全事件，有关主管部门应当依法启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并及时向社会发布与公众有关的警示信息。

第二十四条 国家建立数据安全审查制度，对影响或者可能影响国家安全的数据处理活动进行国家安全审查。

依法作出的安全审查决定为最终决定。

第二十五条 国家对与维护国家安全和利益、履行国际义务相关的属于管制物项的数据依法实施出口管制。

第二十六条 任何国家或者地区在与数据和数据开发利用技术等有关的投资、贸易等方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。

第四章 数据安全保护义务

第二十七条 开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取相应的技术措施和其他必要措施，保障数据安全。利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任。

第二十八条 开展数据处理活动以及研究开发数据新技术，应当有利于促进经济社会发展，增进人民福祉，符合社会公德和伦理。

第二十九条 开展数据处理活动应当加强风险监测，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，按照规定及时告知用户并向有关主管部门报告。

第三十条 重要数据的处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。

风险评估报告应当包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

第三十一条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

第三十二条 任何组织、个人收集数据，应当采取合法、正当的方式，不得窃取或者以其他非法方式获取数据。

法律、行政法规对收集、使用数据的目的、范围有规定的，应当在法律、行政法规规定的目的和范围内收集、使用数据。

第三十三条 从事数据交易中介服务的机构提供服务，应当要求数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录。

第三十四条 法律、行政法规规定提供数据处理相关服务应当取得行政许可的，服务提供者应当依法取得许可。

第三十五条 公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据，应当按照国家有关规定，经过严格的批准手续，依法进行，有关组织、个人应当予以配合。

第三十六条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供数据的请求。非经中华人民共和国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

第五章 政务数据安全与开放

第三十七条 国家大力推进电子政务建设，提高政务数据的科学性、准确性、时效性，提升运用数据服务经济社会发展的能力。

第三十八条 国家机关为履行法定职责的需要收集、使用数据，应当在其履行法定职责的范围内依照法律、行政法规规定的条件和程序进行；对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供。

第三十九条 国家机关应当依照法律、行政法规的规定，建立健全数据安全管理制度，落实数据安全保护责任，保障政务数据安全。

第四十条 国家机关委托他人建设、维护电子政务系统，存储、加工政务数据，应当经过严格的批准程序，并应当监督受托方履行相应的数据安全保护义务。受托方应当依照法律、法规的规定和合同约定履行数据安全保护义务，不得擅自留存、使用、泄露或者向他人提供政务数据。

第四十一条 国家机关应当遵循公正、公平、便民的原则，按照规定及时、准确地公开政务数据。依法不予公开的除外。

第四十二条 国家制定政务数据开放目录，构建统一规范、互联互通、安全可控的政务数据开放平台，推动政务数据开放利用。

第四十三条 法律、法规授权的具有管理公共事务职能的组织为履行法定职责开展数据处理活动，适用本章规定。

第六章 法律责任

第四十四条 有关主管部门在履行数据安全监管职责中，发现数据处理活动存在较大安全风险的，可以按照规定的权限和程序对有关组织、个人进行约谈，并要求有关组织、个人采取措施进行整改，消除隐患。

第四十五条 开展数据处理活动的组织、个人不履行本法第二十七条、第二十九条、第三十条规定的数据安全保护义务的，由有关主管部门责令改正，给予警告，可以并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

违反国家核心数据管理制度，危害国家主权、安全和发展利益的，由有关主管部门处二百万元以上一千万元以下罚款，并根据情况责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；构成犯罪的，依法追究刑事责任。

第四十六条 违反本法第三十一条规定，向境外提供重要数据的，由有关主管部门责令改正，给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；情节严重的，处一百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款。

第四十七条 从事数据交易中介服务的机构未履行本法第三十三条规定的义务的，由有关主管部门责令改正，没收违法所得，处违法所得一倍以上十倍以下罚款，没有违法所得或者违法所得不足十万元的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第四十八条 违反本法第三十五条规定，拒不配合数据调取的，由有关主管部门责令改正，给予警告，并处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

违反本法第三十六条规定，未经主管机关批准向外国司法或者执法机构提供数据的，由有关主管部门给予警告，可以并处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处一万元以上十万元以下罚款；造成严重后果的，处一百万元以上五百万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上五十万元以下罚款。

第四十九条 国家机关不履行本法规定的数据安全保护义务的，对直接负责的主管人员和其他直接责任人员依法给予处分。

第五十条 履行数据安全监管职责的国家工作人员玩忽职守、滥用职权、徇私舞弊的，依法给予处分。

第五十一条 窃取或者以其他非法方式获取数据，开展数据处理活动排除、限制竞争，或者损害个人、组织合法权益的，依照有关法律、行政法规的规定处罚。

第五十二条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 附 则

第五十三条 开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

在统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。

第五十四条 军事数据安全保护的办法，由中央军事委员会依据本法另行制定。

第五十五条 本法自2021年9月1日起施行。

编 辑： 刘 冬

责 编：余 晨

<< 返回首页

打印本页 关闭窗口 返回顶部

EXHIBIT 2

Contents

Chapter I: General Provisions

Article 1: This Law is formulated for the purpose of regulating data processing, safeguarding data security, promoting the development and use of data, protecting the lawful rights and interests of individuals and organizations, and preserving state sovereignty, security, and development interests.

Article 2: This Law applies to data processing activities and security regulations carried out within the territory of the People's Republic of China.

Those who carry out data processing activities outside the territory of the People's Republic of China that compromise the national security of the territory of the People's Republic of China, the public interest, or the lawful rights and interests of individuals and organizations shall be held legally liable in accordance with the law.

Article 3: "Data" as used in this Law refers to any record of information in electronic or other forms.

Data processing includes the collection, storage, use, processing, transmission, provision, and disclosure of data.

Data security means that necessary measures have been adopted to ensure that data is effectively protected and lawfully used, as well as having the capacity to ensure a sustained state of security.

Article 4: In the maintenance of data security, the overall national security perspective shall be adhered to, data security governance systems shall be established and complete, and the capability for data security shall be enhanced.

Article 5: The central leading body for national security is responsible for decision-making, deliberating and coordinating the nation's data security work; researching, drafting, and guiding the implementation of the national data security strategy and related major policy directives; planning and coordinating significant matters and important work in national data security; and establishing a coordination mechanism for national data security work.

Article 6: Each region and department is responsible for the data collected and produced in the work of that region or department and for data security.

Regulatory departments such as those for industries, telecommunications, communications, finance, natural resources, health, education, science and technology shall undertake data security regulatory duties in the corresponding sector.

Public security organs, state security organs, and so forth shall, in accordance with the provisions of this Law, relevant laws, and administrative regulations, undertake data security regulation duties within the scope of their duties.

The State internet information departments shall assume the responsibility for the overall coordination of cyber data security and relevant regulatory efforts in accordance with this Law, relevant laws, and administrative regulations.

Article 7: The State shall protect the rights and interests of individuals and organizations with regards to data; encourage the lawful, reasonable, and effective use of data; ensure the orderly and free flow of data in accordance with the law; and promote the development of a digital economy with data as a key factor.

Article 8: When carrying out data processing activities, one shall abide by laws and regulations, respect social norms and ethics, comply with commercial and professional ethics, be honest and trustworthy, perform obligations to protect data security, and assume social responsibility, and shall neither compromise national security, the public interest, or the lawful rights and interests of any individual and organization.

Article 9: The State shall support the development of publicity and dissemination of knowledge on data security, raise the awareness and level of data security protections of the entire society, push the relevant departments, industry organizations, scientific research bodies, enterprises, and individuals to jointly participate in efforts to protect data security, and form a positive environment for the entire society to jointly maintain data security and promote development.

Article 10: In accordance with their articles of association, relevant industry organizations shall draft a code of conduct and group standards on data security in accordance with the law, strengthen industry self-regulation, guide members in strengthening data security protection, improve the level of data security protection, and promote the healthy development of the industry.

Article 11: The State shall actively develop international exchanges and cooperation in fields such as data security governance and data development and use, participate in the drafting of international rules and standards for data security, and promote the secure and free cross-border flow of data.

Article 12: All individuals and organizations have the right to file complaints or reports to the relevant departments regarding violations of the provisions of this Law. Departments receiving complaints or reports shall handle them promptly and in accordance with the law.

The relevant regulatory departments shall preserve the confidentiality of the relevant information of the complainant or informant and protect the lawful rights and interests of the complainant or informant.

Chapter II: Data Security and Development

Article 13: The State shall make overall plans for development and security, persisting using the development and use of data and industry development to promote data security, and using data security to ensure the development and use of data and industry development.

Article 14: The State shall implement a big data strategy, advancing the establishment of data infrastructure, and encouraging and supporting innovative applications of data in each industry and field.

The people's governments at the provincial level or higher shall incorporate the development of the digital economy in the people's economic and social development plans for that level, and draft development plans for the digital economy as needed.

Article 15: The State shall support the development and use of data to increase the level of smart technology in public services. The provision of smart public services shall fully consider the needs of the elderly and persons with disabilities to avoid creating obstacles in their daily lives.

Article 16: The State shall support research into data use and development and data security technology, encourage the promotion and commercial innovation in areas such as data use and development and data security, and foster and develop data use and development, data security products, and industrial systems.

Article 17: The State shall promote the establishment of a system of standards for data use and development technologies and data security. The State Council departments in charge of standardization and other relevant State Council departments shall, within their respective duties, organize the formulation and appropriate revision of standards related to technology and products for the development and utilization of data and data security. The State shall support enterprises and social groups, educational or research bodies and so forth to participate in the drafting of standards.

Article 18: The State shall promote the development of services such as data security testing, assessment, and certification, and support professional institutions in carrying out data security testing, assessment, certification, and other service activities in accordance with the law.

The State shall support relevant departments, industry organizations, enterprises, educational or scientific research bodies, relevant professional bodies, and so forth in carrying out collaboration in areas such as data security risk assessments, prevention, and handling.

Article 19: The State shall establish and complete management systems for data exchanges, regulate data exchange conduct, and cultivate data exchange markets.

Article 20: The State shall support educational and scientific research bodies, enterprises, and so forth, in carrying out education and training related to data use and development and data security, employing diverse methods to cultivate professional data use and development and data security talent, and promote professional exchanges.

Chapter III: Data Security Systems

Article 21: The State shall establish a hierarchical classification system for data protection and implement hierarchical classification protection of data based on the importance of the data in economic and social development, as well as the extent of compromise to national security, the public interest, or the lawful rights and interests of individuals or organizations that would be caused once the data is altered, destroyed, leaked, or illegally obtained or used. The State's mechanism for coordinating data security

work plans and coordinates the relevant departments' drafting of catalogs of important data and strengthen protections of important data.

Data related to national security, the lifeline of the national economy, important aspects of people's livelihoods, and major public interests are core data of the State, and a more stringent management system shall be implemented.

Each region and department shall determine a catalog of important data within that region and department and corresponding industries and sectors on the basis of the hierarchical classification protection system, and carry out key protection for data entered in the catalog.

Article 22: The State shall establish uniform, highly effective, and authoritative systems for data security risk assessment, reporting, information sharing, monitoring, and early warnings. The State's mechanism for coordinating data security work is to plan and coordinate relevant departments to strengthen the acquisition, analyses, assessment, and early warnings for information on data security risks.

Article 23: The State shall establish a data security emergency response and handling system. Relevant regulatory departments shall initiate emergency response plans in accordance with the law when data security incidents occur, adopting the corresponding emergency response and handling measures to prevent the compromise from increasing, eliminating security risks, and promptly issuing relevant alerts to the public.

Article 24: The State shall establish systems for data security reviews and conduct national security reviews of data processing activities that impact or may impact national security.

Security review decisions made in accordance with the law are final decisions.

Article 25: The State shall implement export controls on data that are controlled items related to maintaining national security and performing international obligations in accordance with the law.

Article 26: Where any nation or region employs discriminatory, restrictive, or other similar measures against the People's Republic of China in terms of areas such as investment or trade in data and technology for the data use and development, the People's Republic of China may employ equal measures against that nation or region based on the actual circumstances.

Chapter IV: Data Security Protection Obligations

Article 27: The carrying out of data processing activities shall be done in accordance with the laws and regulations, establishing and completing data security management systems for the entire process, organizing and carrying out education on data security, and employing corresponding technical measures and other necessary measures to safeguard data security. The use of the internet or other information networks to carry out data processing activities shall be done on the basis of the multi-level protection system for cybersecurity, and the data security protection obligations described above shall be carried out.

Those processing important data shall clearly designate a person in charge of data security and data security management bodies to implement data security protection responsibilities.

Article 28: The carrying out of data processing activities, as well as research into new technology for developing data, shall be conducive to promoting economic development, improve the well-being of the people, and comply with social norms and ethics.

Article 29: The carrying out of data processing activities shall strengthen risk monitoring, and when data security flaws, vulnerabilities, or other risks are found, remedial measures shall be immediately adopted; when data security incidents occur, measures for handling shall be immediately adopted, users shall be promptly notified as required, and reports shall be made to the relevant regulatory departments.

Article 30: Those processing important data shall periodically carry out risk assessments of their data processing activities as required, and send risk assessment reports to the relevant regulatory departments.

Risk assessment reports shall include the types and amounts of important data being processed, the circumstances of the data processing activities, and the data risks faced and their countermeasures.

Article 31: The provisions of the *Cybersecurity Law of the People's Republic of China* are applicable to the security management for exporting of data from the territory that was collected or produced by critical information infrastructure operators inside the territory of the People's Republic of China; security management measures for the export of important data from the territory that was collected and generated by data processors during operations within the territory of the People's Republic of China shall be formulated by the national Cyberspace Administration of China in conjunction with relevant departments of the State Council.

Article 32: Any organization or individual collecting data shall adopt lawful and appropriate methods and must not steal or obtain data through other unlawful means.

Where laws and administrative regulations contain provisions on the purpose or scope of data collection and use, data is to be collected or used within the purpose and scope provided for in those laws and administrative regulations.

Article 33: The provision of services by institutions engaged in data exchange intermediary services shall require the party providing the data to explain the source of the data and shall review and verify the identity of both parties of the exchange, and keep records of the verifications and exchange.

Article 34: Where laws and administrative regulations provide that permits shall be acquired for the provision of services related to data processing, service providers shall obtain permits in accordance with the law.

Article 35: Public security organs and state security organs collecting data as necessary to lawfully maintain national security or investigate crimes shall do so in accordance with relevant state provisions and strict approval procedures, and relevant organizations and individuals shall cooperate.

Article 36: The competent authority of the People's Republic of China shall handle requests for the provision of data from foreign judicial or law enforcement authorities in accordance with relevant laws and international treaties and agreements concluded or acceded to by the People's Republic of China, or in accordance with the principle of equality and reciprocity. Without the approval of the competent authority of the People's Republic of China, domestic organizations and individuals shall not provide data stored within the territory of the People's Republic of China to foreign judicial or law enforcement authorities.

Chapter V: Security and Public Availability of Government Data

Article 37: The State shall strongly promote the establishment of an e-government, increase the scientific nature, accuracy, and efficacy of government affairs data, and increase the ability to use data in serving economic and social development.

Article 38: The collection or use of data by State organs to perform their statutory duties shall be carried out in accordance with the conditions and procedures provided by laws and administrative regulations within the scope of their statutory duties; personal privacy, personal data, trade secrets, confidential business data and other data shall be kept confidential in accordance with the law, and shall not be leaked or unlawfully provided to others.

Article 39: State organs shall establish and complete data security management systems, implement responsibility for data security protection, and ensure the security of government affairs data in accordance with the provisions of laws and administrative regulations.

Article 40: State organs entrusting others to establish or maintain an e-government system or to store or process government data shall go through strict approval procedures, and shall oversee the performance of data security protection obligations by the entrusted parties. The entrusted party shall perform data security protection obligations in accordance with the laws, regulations, and contractual agreements, and must not store, use, leak, or provide others with government data without authorization.

Article 41: State organs shall abide by the principles of justice, fairness, and convenience for the people to promptly and accurately disclose government data as required, except where it may not be disclosed in accordance with the law.

Article 42: The State shall create a catalog of available government data, establish a uniform and standardized, interconnected, secure and controllable platform for accessing government data, and promote the use of available government affairs data.

Article 43: The provisions of this Chapter are applicable to the carrying out of data processing activities by organizations authorized by laws or regulations to have public affairs management duties in order to perform their statutory duties.

Chapter VI: Legal Liability

Article 44: Where relevant regulatory departments performing data security oversight and management duties discover that data processing activities carry larger security risks, they can interview the organizations and individuals in accordance with the prescribed authority and procedures, and require the relevant organizations or individuals to adopt measures to correct or eliminate the risks.

Article 45: Where organizations or individuals carrying out data processing activities fail to perform the data security protection obligations prescribed by Articles 27, 29, and 30 of this Law, the relevant regulatory departments shall order corrections and give warnings, and may issue a fine between RMB 50,000 and 500,000 or issue a fine between RMB 10,000 and 50,000 to directly responsible managers and other directly responsible personnel; for those who refuse corrections or where a large data leak or other serious consequences are caused, a fine between RMB 500,000 and 2,000,000 shall be issued, and they may be ordered to cease relevant operations or suspend operations for corrections, and their relevant business permits or licenses may be cancelled, and the directly responsible managers and other directly responsible personnel shall be issued a fine between RMB 50,000 and 200,000.

For those who violate the State's core state data management system, compromising the nation's sovereignty, security, or development interests, the relevant regulatory departments shall issue a fine between RMB 2,000,000 and 10,000,000, and according to the circumstances, they may be ordered to cease relevant operations or suspend operations for corrections, and their relevant business permits or licenses may be cancelled; where it constitutes a crime, criminal liability shall be pursued in accordance with the law.

Article 46: Where organizations or individuals violate the provisions of Article 31 of this Law by providing important data overseas, the relevant regulatory departments shall order corrections and give warnings, and may issue a fine between RMB 100,000 and 1,000,000 or issue a fine between RMB 10,000 and 50,000 to directly responsible managers and other directly responsible personnel; where the circumstances are serious, a fine between RMB 1,000,000 and 10,000,000 shall be issued, and they may be ordered to cease relevant operations or suspend operations for corrections, and their relevant business permits or licenses may be cancelled, and the directly responsible managers and other directly responsible personnel shall be issued a fine between RMB 100,000 and 1,000,000.

Article 47: Where institutions engaged in data exchange intermediary services fail to perform the obligations in Article 33 of this Law, the relevant regulatory departments shall order corrections, confiscate the unlawful gains, and issue a fine between 1 and 10 times the value of the unlawful gains, or a fine between RMB 100,000 and 1,000,000 shall be issued where there are no unlawful gains or the unlawful gains are less than RMB 100,000, and they may be ordered to cease relevant operations, suspend operations for corrections or their related business permits or licenses may be cancelled; a fine between RMB 10,000 and 100,000 shall be issued to the directly responsible managers and other directly responsible personnel.

Article 48: For those who violate Article 35 of this Law due to the refusal to cooperate in the collection of data, the relevant regulatory departments shall order corrections and give warnings, issue a fine between RMB 50,000 and 500,000, and issue a fine between RMB 10,000 and 100,000 to directly responsible managers and other directly responsible personnel.

For those who violate Article 36 of this Law due to the provision of data to foreign justice or law enforcement authorities without the approval of the organs in charge, the relevant regulatory departments shall give warnings, may issue a fine between RMB 100,000 and 1,000,000, and may issue a fine between RMB 10,000 and 50,000 to directly responsible managers and other directly responsible personnel; where serious consequences result, a fine between RMB 1,000,000 and 5,000,000 shall be issued, and they may be ordered to cease relevant operations, suspend operations for corrections, or their relevant business permits or licenses may be cancelled, and the directly responsible managers and other directly responsible personnel shall be issued a fine between RMB 50,000 and 500,000.

Article 49: Where state organs do not perform obligations to protect data security as prescribed by this Law, the directly responsible managers and other directly responsible personnel shall be issued sanctions in accordance with the law.

Article 50: Where state personnel with duties to regulate data security derelict their duties, abuse their powers or engaged in malpractice for personal gains, they shall be sanctioned in accordance with the law.

Article 51: Those who steal or obtain data by other illegal means, carry out of data processing activities to eliminate or restrict competition, or harm the lawful rights and interests of individuals or organizations shall be punished in accordance with the laws and administrative regulations.

Article 52: Those who violate the provisions of this Law and causes damage to others shall bear civil liability in accordance with the law.

Where violations of the provisions of this Law constitute a violation of public security management, public security administrative sanctions shall be given in accordance with the law; where a crime is constituted, criminal liability shall be pursued in accordance with the law.

Chapter VII: Supplementary Provisions

Article 53: The *State Secrets Protection Law of the People's Republic of China* and other relevant laws and administrative regulations are applicable to the carrying out of data processing activities that involve state secrets.

The carrying out of data processing activities in statistics or archival work, or where personal data shall also comply with relevant laws and administrative regulations.

Article 54: Military data security measures shall be separately drafted by the Central Military Commission on the basis of this Law.

Article 55: This Law is to be implemented beginning on September 1, 2021.

TRANSPERFECT

DATE OF TRANSLATION:	9-September-21
ELECTRONIC FILE NAME:	Data Security Law of the People□s Republic of China
SOURCE LANGUAGE:	Chinese
TARGET LANGUAGE:	English
TRANSPERFECT JOB ID:	US1090627

TransPerfect is globally certified under the standards ISO 9001:2015 and ISO 17100:2015. This Translation Certificate confirms the included documents have been completed in conformance with the Quality Management System documented in its ISO process maps and are, to the best knowledge and belief of all TransPerfect employees engaged on the project, full and accurate translations of the source material.

TCert v. 2.0

EXHIBIT B

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

MAXELL HOLDINGS, LTD.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Civil Action No.: 6:21-cv-00347-ADA**
	)	
AMPEREX TECHNOLOGY LIMITED,	)	
	)	
Defendant.	)	

DECLARATION OF HANJING XIAO IN SUPPORT OF DEFENDANT'S MOTION TO EXTEND DEADLINE FOR TECHNICAL DOCUMENT PRODUCTION

I, Hanjing Xiao, hereby declare as follows:

1. I am over 18 years old and am a citizen of the People's Republic of China. I currently reside in Ningde City, Fujian Province, China.

2. I submit this declaration in support of Defendant Amperex Technology Limited's ("ATL") Motion to Extend Deadline for Technical Document Production. I have personal knowledge as to the facts stated in this declaration, and all facts stated are true and correct, to the best of my knowledge.

3. I am currently the corporate counsel of ATL. I have been in this role at ATL since 2015.

4. As the corporate counsel of ATL, my duties include providing legal advice on sales and procurement contracts and litigation matters.

5. Under this Court's Order Governing Proceedings – Patent Case and the deadlines in the Court's Scheduling Order, ATL has been collecting "technical documents, including software where applicable, sufficient to show the operation of the accused product(s)" to be produced in this litigation on September 10, 2021. However, before it could complete its

document collection, ATL became aware of the pending Data Security Law of the People's Republic of China ("DSL").

6. ATL immediately sought legal guidance from its Chinese counsel Fanghua Liu regarding its obligations under the DSL.

7. ATL understands from it counsel that the DSL applies to ATL because all of the technical documents required by the Court to be produced are located and held in mainland China, primarily at ATL's Ningde location. Because the data is located in the territory of China and with ATL's mainland China affiliate, ATL understands from its counsel that the DSL prevents those data to be transferred outside of the territory of China.

8. ATL is also informed by counsel that the consequences of violating the DSL can be serious including severe monetary fines and suspension of business license, among others.

9. Under the advice of its counsel, ATL has immediately sought approval and guidance from the competent authorities in China. In particular, on August 30th and 31st, 2021, ATL called Ningde Cyberspace Administration, Cyberspace Administration of China, and Intellectual Property Bureau of Ningde City with regard to the approval procedure for data exportation. ATL has also contacted the Intellectual Property Bureau of Ningde City to obtain permission to produce the relevant data to this Court and Plaintiff..

10. However, the Cyberspace Administration of China responded on August 31, 2021 that the DSL is a new legislation, and the government is in the process of formulating relevant rules and regulations on the cross-border data transfer and approval procedure.

11. The Intellectual Property Bureau of Ningde City responded on August 31, 2021 that it is not in a position to approve ATL's application for data exportation because it is not the competent authority of the DSL.

12. As of today, ATL has not received any permission or formal instructions from any Chinese authorities with regard to the data transfer request sought by ATL under the DSL.

13. ATL and Maxell have engaged in ongoing settlement discussions, and Maxell has had access to and investigated ATL's physical products for more than one year.

I declare under penalty of perjury under the laws of the United States and the State of Texas that the foregoing is true and correct.

Executed this 10th day of September 2021, in Ningde City, Fujian Province, China.

By: _____
Hanjing Xiao